UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
v.	:	15 Cr. 866 (WHP)
ROGER THOMAS CLARK, a/k/a "Variety Jones," a/k/a "Cimon," a/k/a "VJ," a/k/a "Plural of Mongoose,"	:	
Defendant.	:	

MEMORANDUM OF LAW OF THE UNITED STATES OF AMERICA IN OPPOSITION TO DEFENDANT'S MOTIONS TO SUPPRESS EVIDENCE AND OBTAIN DISCOVERY

GEOFFREY S. BERMAN
United States Attorney for the
Southern District of New York
One St. Andrew's Plaza
New York, New York 10007

Michael D. Neff
Vladislav Vainberg
Eun Young Choi
Assistant United States Attorneys
Of Counsel

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

Rules and Statutes

I. PRELIMINARY STATEMENT

From January 2011 to October 2013, the Silk Road was a massive, online illicit black market that was used by thousands of drug dealers and other criminals to distribute illegal drugs and other illicit goods and services to over 100,000 buyers, and to launder hundreds of millions of dollars derived from those unlawful transactions. Defendant Roger Thomas Clark ("Clark" or the "defendant") was an advisor and mentor to Ross Ulbricht—the creator, owner, and operator of Silk Road. Clark advised Ulbricht on all aspects of Silk Road's operations, including urging Ulbricht to commission a murder-for-hire of someone who had stolen from Silk Road. The Government arrested Ulbricht while he was logged into Silk Road as its administrator. Ulbricht's computer (the "Ulbricht Laptop") contained chats between Ulbricht and his employees, including with Clark about the day-to-day management of Silk Road and how to evade law enforcement.

Clark now moves to suppress virtually all of the Government's evidence, including (a) the contents of various Silk Road servers; (b) evidence from Ulbricht's home, devices, and electronic accounts; (c) the contents of a third party's email account; (d) devices seized from Clark's residence in Thailand, by the Royal Thai Police, in connection with Clark's 2015 arrest; and (e) Clark's post-arrest statements, both oral and written.

Most of Clark's 39 suppression motions rely, directly or derivatively, on one central claim: The Government (purportedly) violated the Fourth Amendment by not obtaining a warrant to review a copy of the Silk Road server legitimately seized and accessed by Icelandic law enforcement in Iceland (the "Icelandic Server"), in response to a diplomatic request from the United States.

Clark's central claim is wrong for at least four reasons. *First*, under binding precedent, Clark cannot invoke the Fourth Amendment for his claims, because—as a Canadian citizen then

residing in Thailand—he lacked voluntary, substantial connections to the United States at the time of the foreign search at issue. *Second*, regardless of Clark's ties to the United States, the Fourth Amendment does not apply abroad, including to the seizure and imaging of the Icelandic Server. *Third*, even if the Fourth Amendment did apply, Clark lacks standing to challenge the search of the Icelandic Server because, among other reasons, he did not own, lease, control, or pay for the Icelandic Server. *Fourth*, even if the Court assumed that Clark had standing, no court has ever adopted Clark's substantive argument: that evidence properly seized and imaged abroad, by foreign law enforcement, is nevertheless subject to the warrant requirement once it crosses the border to be reviewed domestically by U.S. law enforcement. Given the lack of any precedent for this novel (and incorrect) argument, the good-faith exception to the exclusionary rule applies.

In addition to his central claim, Clark seeks to suppress his various post-arrest statements in Thailand, oral and written. But there is simply no basis to do so. Clark was *Mirandized* before both of his oral statements to an HSI Special Agent, and he knowingly and voluntarily waived his rights. As for his written statements, they were not in response to any questioning at all. Rather, Clark made a strategic choice to contact the same HSI Special Agent as part of his unsolicited bid for immunity.

Clark also asserts that his devices, which were seized from his home in Thailand during his arrest, should be suppressed because he was allegedly coerced by Thai police into signing a form consenting to their seizure. But Clark conflates two issues. The Government does not need, and is not relying on, this consent form. As for the devices, the United States submitted a request to the Kingdom of Thailand to arrest a defendant in a sophisticated cybercrime case, and the Royal Thai Police seized Clark's devices during the course of executing his arrest—an entirely unsurprising fact in a case involving computer crime. The Government later obtained a search

warrant in this District for those devices, amply supported by probable cause (and not relying at all on the consent form).

Finally, Clark lodges 12 meritless discovery requests, resurrecting a fishing expedition previously, and unsuccessfully, pursued by Ulbricht. These requests should all be denied, as well.

II. FACTUAL BACKGROUND[1]

A. The Silk Road Website

From January 2011 until October 2, 2013, the "Silk Road" website hosted a sprawling black-market bazaar on the Internet, where illegal drugs and other illicit goods and services were regularly bought and sold by the site's users. Silk Road was an online black market of unprecedented scope. By the time it was shuttered in October 2013, more than 13,000 offerings were listed on its homepage for illegal drugs of virtually every variety. A wide variety of other illicit goods and services were sold on the site as well, including fake IDs and passports, computer-hacking tools and services, counterfeit goods and pirated media, criminal guidebooks and instruction manuals, and money laundering services. In total, more than 1.5 million transactions were conducted over the Silk Road, involving more than 100,000 buyer accounts and nearly 4,000 seller accounts. Those transactions had a total value of more than $213 million in U.S. currency, and nearly 95% of those sales (approximately $183 million worth) were for illegal drugs. The buyers and sellers involved in these transactions were spread across the world.

[1] These facts are drawn, in substantial part, from the public record accumulated through other Silk Road cases in this District (and one appeal in this Circuit), including those of Ross William Ulbricht, Peter Phillip Nash, Andrew Michael Jones, and Gary Davis. *See, e.g.*, *United States v. Ross William Ulbricht*, 14 Cr. 68 (LGS); *United States v. Peter Phillip Nash, Andrew Michael Jones, and Gary Davis*, 13 Cr. 850 (JMF). Ulbricht proceeded to trial in 2015 before Judge Forrest and ultimately appealed his conviction and sentence to the Second Circuit. In a 139-page opinion, the Second Circuit affirmed Ulbricht's conviction and sentence in all respects. *See United States v. Ulbricht*, 858 F.3d 71, 82 (2d Cir. 2017), *cert. denied*, 138 S. Ct. 2708 (2018). Nash, Jones, and Davis each pleaded guilty.

Unlike mainstream commerce websites, Silk Road was only accessible on the Tor network. The Tor network is a special network of computers on the Internet, distributed around the world, that is designed to conceal the true Internet protocol addresses (or "IP addresses") of the computers on the network and, thereby, enhance the anonymity of network's users.[2] Tor also allows websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, referred to as "hidden services." Such "hidden services" operating on Tor have complex web addresses ending in ".onion." Such addresses can only be accessed using special Tor web browser software.

The only form of payment accepted on Silk Road was Bitcoin—a decentralized form of electronic currency, existing entirely on the Internet and not in any physical form. Bitcoin is designed to be as anonymous as cash. Although Bitcoin has known legitimate uses, it is particularly attractive to cybercriminals and money launderers, because of its anonymity.

Silk Road charged a commission for every transaction conducted by its users, generally 8 to 15 percent. During its operation, Silk Road generated sales revenue totaling over 9.9 million Bitcoins and collected commissions from these sales totaling over 640,000 Bitcoins, worth more than $213 million and $13 million, respectively, based on the prevailing Bitcoin exchange rates when the underlying sales occurred.

B. The Investigation

During the course of its investigation, the FBI New York Field Office located the server hosting the Silk Road website (the Icelandic Server) in or about June 2013. (*See* Decl. of Christopher Tarbell ("Tarbell Decl."), attached as Exhibit C to Mitchell Declaration (Dkt. 34-3),

[2] An IP address is a unique series of numbers, separated by periods, that identifies each device using the Internet Protocol to communicate over a network.

¶ 5). The IP address of the Icelandic Server (the "Icelandic IP Address") was "leaking" from the site due to an apparent misconfiguration of the user login interface by the site administrator—*i.e.*, Ulbricht. (*Id.* ¶¶ 4-8). (Indeed, Ulbricht's own "journal" entry from May 3, 2013, on the Ulbricht Laptop, noted a leaking IP address.)

Based on publicly available information, the Icelandic IP Address was associated with a server housed at a data center operated by a foreign server-hosting company in Iceland. (*Id.* ¶ 9). Accordingly, on June 12, 2013, the United States issued an official request[3] to Iceland for Icelandic authorities to take certain investigative measures with respect to the server, including collecting routing information for communications sent to and from the server, and covertly imaging the contents of the server. The Reykjavik Metropolitan Police ("RMP") provided routing information for the server soon thereafter, which showed a high volume of Tor traffic flowing to the server—further confirming that it was hosting a large website on Tor. Subsequently, after obtaining the legal process required under Icelandic law to search the server, and after consulting with U.S. authorities concerning the timing of the search, the RMP covertly imaged the server on or about July 22, 2013. The FBI was not present or otherwise involved in the imaging of the server, other than consulting with the RMP as to when the imaging should be done. (*Id.* ¶ 12). The RMP shared the results with the FBI on or about July 29, 2013. (*Id.* ¶ 12). Forensic examination of the image by the FBI confirmed that the server was hosting the Silk Road website and contained the contents of the site—including databases of vendor postings, transaction records, and private messages between users—as well as the computer code used to operate the website. (*Id.* ¶ 13).

[3] Although the search warrants in this case refer to the request as a "Mutual Legal Assistance Treaty request," this description is not technically correct, as the United States does not have an MLAT with Iceland. The request was instead an official request to Iceland issued pursuant to the 2001 Council of Europe Convention on Cybercrime and other relevant law of Iceland, and as a matter of comity.

From examining the computer code on the Icelandic Server, the FBI learned of IP addresses of additional servers used in connection with administering the Silk Road website, including a backup server in a Pennsylvania data center. (*Id.* ¶¶ 15-16). The FBI obtained a warrant to search this backup server and a secondary backup server.[4] (*Id.* ¶ 17).

By mid-September 2013, Ulbricht was the Government's lead suspect as the owner and operator of Silk Road, known on the site as "Dread Pirate Roberts," or "DPR." (*Id.* ¶ 18). Accordingly, around that time, the Government obtained several judicially authorized pen registers for the purpose of confirming that Ulbricht was "DPR." (*Id.* ¶ 19). These pen registers authorized the FBI to collect routing data from the Internet service provider ("ISP") account associated with Ulbricht's residence (the "ISP Account"), the wireless router associated with that account (the "Router"), and certain hardware devices that were regularly connecting to the router (the "Devices"). (*Id.* ¶ 19). The data collected through these pen registers (the "Pen Registers") did not include the contents of any communications. (*Id.*). Instead, the data consisted of the IP addresses in contact with the ISP Account, Router, and Devices, along with the dates, times, durations, and other routing information associated with these connections—similar to the data associated with incoming and outgoing phone calls that the Government can obtain with a pen register on a phone line. (*Id.*). On October 1, 2013, in the hours before Ulbricht's arrest, the FBI obtained two search warrants from the United States District Court for the Northern District of

[4] The FBI's analysis of the Icelandic Server yielded IP addresses of other servers associated with the Silk Road site as well, some of which were hosted by U.S.-based providers and some of which were hosted by foreign providers. (*Id.* ¶ 15). The Government obtained the contents of the former through search warrants and obtained the contents of the latter through requests for law enforcement assistance directed to the corresponding foreign countries. (*Id.* ¶ 15). Clark does not make any specific challenge to the searches of these additional servers in his motion beyond moving to suppress virtually all of the evidence obtained following the FBI's analysis of the Icelandic Server as the fruit of a purportedly illegal search.

California—one authorizing a search of Ulbricht's residence, and the other authorizing a search of his computer. (*Id.* ¶ 22).

In April 2015, the FBI obtained a search warrant for the contents of an email account registered in the name of [redacted]. This email account was associated with a Bitcoin account used to convert and launder the proceeds of illegal goods and services sold on Silk Road. In all affidavits supporting warrants obtained subsequent to the review of the Icelandic Server, where the Icelandic Server was mentioned, the FBI disclosed that the Icelandic Server had been located in a foreign country, imaged pursuant to a Mutual Legal Assistance Treaty request, and then provided to the FBI.

C. Ross Ulbricht

The investigation revealed that Ross Ulbricht ("Ulbricht") created, owned, and operated Silk Road. Ulbricht conceived of Silk Road in late 2009 as an "online storefront that couldn't be traced back to me." Once he launched the site, he attempted to attract users to Silk Road by marketing it on various online forums, including forums frequented by Bitcoin users.

Ulbricht oversaw every aspect of the operation of Silk Road from the time he launched the site in early 2011 until his arrest in October 2013. Among other things, Ulbricht was responsible for setting the commission rate for transactions on Silk Road; determining what goods were, and were not, allowed to be sold on Silk Road; enforcing the site's rules, including the ban on offline sales between vendors and customers, designed to avoid Silk Road commissions; maintaining and managing the computer servers and code used to operate and run Silk Road; and managing the day-to-day operations of the site, with the help of his employees whom he hired, supervised, and paid. As Ulbricht put it in one post to the Silk Road community, in response to some users expressing displeasure with the new higher commissions, "Whether you like it or not, I am the

captain of this ship. You are here voluntarily and if you don't like the rules of the game, or you don't trust your captain, you can get off the boat."

Ulbricht was initially identified as the administrator of Silk Road through connections between his personal email account and online posts about Silk Road. After identifying him, agents were able to catch Ulbricht red-handed, arresting him in a public library in San Francisco while he was logged into Silk Road from his laptop, administering the site and talking online with an undercover agent.

Subsequent examination of the Ulbricht Laptop revealed voluminous evidence tying Ulbricht to the creation, ownership, and operation of Silk Road for the length of its existence. This evidence included, among other things, (1) thousands of pages of chat logs with his employees; (2) journal entries describing his ownership and operation of Silk Road; (3) a weekly "to do" list regarding Silk Road–related tasks; (4) a copy of the Silk Road website; (5) a copy of the Silk Road website's database (which included information about Silk Road's users and their transactions); (6) a spreadsheet with information about the servers used to operate Silk Road; (7) the private PGP encryption key that "Dread Pirate Roberts" used to authenticate and encrypt his messages; (8) an expense report spreadsheet, listing expenses and profits related to Silk Road; (9) a spreadsheet listing Ulbricht's assets, which included a reference to Silk Road as an asset valued at approximately $104 million as of June 2012; and (10) scanned copies of identification documents belonging to Silk Road staff members—including Roger Thomas Clark.

Given Silk Road's unprecedented size and scope, Ulbricht could not do everything himself, so he ran the site with the aid of support staff. One member of his staff was Roger Thomas Clark.

D. Roger Thomas Clark

The investigation revealed that Clark—who went by the online nicknames "Variety Jones," "VJ," "Cimon," and "Plural of Mongoose"—was an advisor to Ulbricht about all aspects of Silk Road. The chat logs on the Ulbricht Laptop included over a thousand pages of chats between Ulbricht and "VJ" and "Cimon," which ranged from in or about December 2011 through in or about April 2013. During these chats, Clark advised Ulbricht about, among other topics, security vulnerabilities in the Silk Road site; technical infrastructure; the rules that governed Silk Road users and vendors; the promotion of sales on Silk Road, including the sales of narcotics; and how to evade law enforcement. Clark also assisted with hiring programmers to help improve the infrastructure of, and maintain, Silk Road. Clark also was responsible for gathering information on law enforcement's efforts to investigate Silk Road. And Clark advised Ulbricht on how to protect the Silk Road empire; for instance, when a Silk Road staff member was suspected of stealing $350,000 in Bitcoin from the site, Clark suggested to Ulbricht that Ulbricht commission a murder-for-hire. Ulbricht took that suggestion.[5]

In a journal entry dated 2011, Ulbricht wrote about the Silk Road's successful first year in operation, and in the following excerpt, described how "Variety Jones" provided him with significant advice and assistance with Silk Road:[6]

> Around this time, Variety Jones showed up. This was the biggest and strongest willed character I had met through the site thus far. He quickly proved to me that he had value by pointing out a major security hole in the site I was unaware of. It was an attack on bitcoind. We quickly began discussing every aspect of the site as well as future ideas. He convinced me of a server configuration paradigm that gave me the confidence to be the sole server administrator and not work with someone

[5] Ultimately, Ulbricht agreed to pay a Silk Road vendor, "Nob," $80,000 to kill the Silk Road staff member who had stolen the money. Unbeknownst to Ulbricht, "Nob" was an undercover law enforcement agent. No murder in fact occurred.

[6] All quoted journal entries and chat logs are provided verbatim herein, including any errors in spelling, grammar and punctuation.

> else at all. He has advised me on many technical aspect of what we are doing, helped me speed up the site and squeeze more out of my current servers. He also has helped me better interact with the community around Silk Road, delivering proclamations, handling troublesome characters, running a sale, changing my name, devising rules, and on and on. He also helped me get my head straight regarding legal protection, cover stories, devising a will, finding a successor, and so on. He's been a real mentor.

As noted in this journal entry, Clark advised Ulbricht on developing a "cover story" to make it appear as though Ulbricht had sold Silk Road. During a chat in December 2011, Clark advised Ulbricht to limit the number of people who knew that he owned and operated Silk Road, stating, "remember - someday it would be very valuable information who started SR." Clark asked whether Ulbricht had disclosed to anyone that he was involved in Silk Road. Ulbricht said that there were two people, but he had recently told them he had sold the site. The next month, Clark asked Ulbricht whether he had seen the movie *The Princess Bride*, and whether he knew the history of the "Dread Pirate Roberts." Clark explained the legend of the character "Dread Pirate Roberts," how "over the years, a new one would take the name, and the old one would retire." Clark urged Ulbricht to change his name on Silk Road "from Admin, to Dread Pirate Roberts" to "clear your old trail – to be honest, as tight as you play things, you are the weak link from those two prev contacts." Ulbricht took this advice. Less than a month later, in a post on the Silk Road Forum, the "Admin" account—known to be the chief administrator account for Silk Road—announced that "my new name is: Dread Pirate Roberts." At the time of Ulbricht's arrest, Ulbricht was logged into the Silk Road website as the "Dread Pirate Roberts" administrator account from his laptop.

Ulbricht paid Clark for his services. One file recovered from the Ulbricht Laptop was a spreadsheet file labeled "sr_accounting," reflecting various Silk Road related expenses. These included several references to payments to Clark (under the online pseudonym "cimon"), including payments of approximately: (1) $93,150 in United States currency on or about November 16, 2012;

(2) $50,000 in United States currency on or about May 7, 2013; and (3) $57,000 in United States currency on or about July 3, 2013.

Chat logs between Ulbricht and various co-conspirators make clear that Ulbricht required staff members to provide a scanned copy of personal identification documents, in order to work for him as part of the Silk Road enterprise. The Ulbricht Laptop contained a folder labeled "IDs," which contained a number of encrypted image files, each of which was entitled with the online pseudonym of a Silk Road co-conspirator. One encrypted file, entitled "cimon.jpg," contains a color photograph of a Canadian passport for Roger Thomas Clark.[7]

E. Clark's Arrest, Post-Arrest Statements, and Thai Extradition Proceedings

On or about December 3, 2015, Clark was arrested at his residence in Thailand, and in connection with his arrest, the Royal Thai Police seized various electronic devices from his residence. Those devices were later transported to this District, where a judicially authorized warrant was obtained to search them.[8]

In the days and months after his arrest, the defendant made a series of oral and written statements, which he now moves to suppress:[9]

1. On or about December 4, 2015, Clark met with HSI Special Agent Michael Joseph in a Thai courthouse. Special Agent Joseph advised Clark of his rights, both orally and in writing. Clark acknowledged his rights, signed a *Miranda* form (Ex. A), and agreed to speak with Special Agent Joseph. In substance and in part, Clark stated that he prefers to be called "Mongoose," and he had been living in Thailand for over three years. He also stated that he had a good understanding of the American judicial process. Although the interview was cut short because Clark needed to be taken to a holding cell, Clark agreed to speak again with Special Agent Joseph in the future.

[7] Clark was also a seller on Silk Road—he sold marijuana seeds.

[8] That search is ongoing, as the defendant encrypted his three laptop computers.

[9] There is one additional post-arrest statement, which it appears the defendant has *not* moved to suppress, which involves a consent form that he alleges the Thai police made him sign in connection with his arrest. The Government is not seeking to use that form or the statements in it.

2. In a letter from in or around March 2016, Clark wrote that he had expected to see Special Agent Joseph in December or January, and added that "I am not willing to meet with anyone but you." Clark expressed hope that he and Special Agent Joseph "could enter into some informal discussions," and added that because he had not heard from his lawyer in well over two months, "let's assume I'm representing myself until I inform you otherwise. . . . I'm looking forward to you dropping by for a chat in the near future."

3. On or about May 11, 2016, Clark met with HSI Special Agent Michael Joseph at a Thai prison. Special Agent Joseph again advised Clark of his rights, both orally and in writing. Clark acknowledged his rights, signed a *Miranda* form (Ex. B), and agreed to speak with Special Agent Joseph. In substance and in part, Clark stated that it was still okay to call him "Mongoose"; that he is a pacifist who has never been involved in any violence; that he had a new attorney but lacked contact information for counsel; that he desired an offer of immunity in exchange for his cooperation; and that, once he beat the charges, he believes he can help the United States by providing information about a purportedly rogue FBI agent. Clark agreed to speak with Special Agent Joseph again one week later.

4. On or about May 18, 2016, Clark wrote to Special Agent Joseph that: "I have develope [sic] the ability to de-anonymized [sic] specific, targeted subjects IP address using Tor, employing a method compatible with both current and the upcoming next generation toward servicing, and which will remain effective well into the next decade. I will allow 10 days for American measured response."

5. On or about June 15, 2018, Clark was extradited from Thailand and made extremely limited oral statements to an FBI Special Agent upon arrival at the courthouse at 500 Pearl Street. Clark was read his rights, but declined to sign the form, noting that he had been awake for 40 hours and had a poor experience in Thailand with signing documents. Clark stated, in substance and in part, that he was looking forward to quitting smoking due to the no-smoking policy in U.S. jails. When advised that he would still likely be able to obtain cigarettes in detention, Clark expressed that, though it was ironic for someone in his position, he did not like to use black markets.

The Government has no intention of using the fifth statement (Clark's statement at 500 Pearl Street). However, the Government does intend to use statements one through four.

Finally, during the course of Thai extradition proceedings, Clark testified under oath and made several statements that (based on a draft translation) are flatly inconsistent with the Declaration that he has filed in connection with his instant motions, including:

- At the time he was arrested (*i.e.*, before he received the allegations against him), he "had no knowledge" regarding Silk Road and "did not have any involvement with this website"; and

- At the time he was arrested (*i.e.*, before he received the allegations against him), he "had no knowledge" regarding Ross Ulbricht, and was not associated with Ulbricht.

See Ex. C (Transcript of Extradition Hearing in Thailand, pp. 4, 7 (in English version)). Clark was ultimately ordered extradited, arrived in this District in June 2018, and is set for trial in May 2020.

F. Clark's Motions to Suppress

While in Thailand, Clark disclaimed—under oath—any involvement in Silk Road. Now, he claims to have "devot[ed] the majority of [his] time to participate with DPR in running Silk Road." (Dkt. 35 (Clark Decl. ¶ 8)). He also claims, without any evidence, to have been a part-owner of Silk Road. (*Id.* ¶ 14). He makes such claims in his attempt to knock out virtually all of the Government's documentary and electronic evidence, as he seeks to suppress the following:

- The Silk Road Server Motions: Sixteen suppression motions seek to suppress the contents of various Silk Road servers in Iceland, France, and the United States. These were Silk Road's marketplace, forum, and Bitcoin servers, as well as its backup servers. These servers contain, among other things, transactional data and certain communications between co-conspirators. The contents of the Icelandic and French servers were respectively obtained through formal requests and requests pursuant to Mutual Legal Assistance Treaties ("MLAT") in 2013. The contents of the United States servers were obtained through judicially authorized search warrants in 2013.

- The Ulbricht Motions: Eleven suppression motions seek to suppress evidence seized from Ross Ulbricht's San Francisco residence, Ross Ulbricht's electronic devices (his computer and his Kindle), Ross Ulbricht's electronic accounts (Gmail and Facebook), and pen register data relating to Ross Ulbricht's wireless router, computer, and IP address. The pen register data was obtained pursuant to judicially authorized orders; all other evidence (summarized in this paragraph) was obtained through judicially authorized search warrants.

- The [redacted] Motion: One suppression motion seeks to suppress evidence seized from an email account, [redacted] which was obtained pursuant to a judicially authorized search warrant. This email account was associated

with a Bitcoin account that had been used to convert, into U.S. currency, a portion of the Bitcoin that DPR had paid Clark on Silk Road.

- The Thai Evidence Motions: Seven suppression motions seek to suppress evidence (laptops, thumb drives, a hard drive, and a camera) seized from Roger Thomas Clark's residence in Thailand in connection with his December 3, 2015 arrest there. These devices were seized from Clark's residence, subsequently obtained pursuant to an MLAT request to Thailand, and searched in this District pursuant to a judicially authorized search warrant.

- The Post-Arrest Statement Motions: Two suppression motions seek to suppress four post-arrest statements that Clark made to an HSI Special Agent in Thailand—two sets of oral, *Mirandized* statements (2015 and 2016), and two unsolicited written statements in 2016.

- The SDNY Statement Motion: One suppression motion seeks to suppress Clark's limited, oral statement to an FBI Special Agent in SDNY in 2018, on the date Clark was extradited from Thailand.

- The Residual Motion: The final motion seeks to suppress any evidence obtained directly or indirectly as a result of warrantless searches, in the United States, of Silk Road servers obtained from other countries, including "all the material" on two 4-Terabyte drives, produced in July 2018,[10] that comprised the bulk of discovery in this case.

(Dkt. 32 (Notice of Motion); Dkt. 36 ("Def. Br.")). Clark has also filed 12 discovery requests.

III. THERE WAS NO FOURTH AMENDMENT VIOLATION

Clark seeks suppression of the Icelandic Server's contents on the ground that the server was searched without a warrant in violation of the Fourth Amendment. (Def. Br. 13). As the defendant acknowledges (Def. Br. 13 & n.18), he bears the burden of establishing that the search and seizure of the Icelandic Server violated his own Fourth Amendment rights and that suppression is the appropriate remedy.

Clark fails to establish any Fourth Amendment violation, much less a violation warranting suppression, for at least four independent reasons. First, as a fundamental threshold matter, the

[10] The defense's Notice of Motion states that the date of this production was July 31, 2019. That is a typographical error; in fact, it was produced a year earlier on July 31, 2018.

Fourth Amendment does not apply "to the search and seizure by United States agents of property that is owned by a nonresident alien and located in a foreign country." *United States v. Verdugo-Urquidez*, 494 U.S. 259, 261 (1990). Clark, a Canadian citizen who resided in Thailand at the time of the search and seizure of the Icelandic Server in Iceland, did not establish any voluntary connections to the United States, much less the substantial connections necessary to invoke the Fourth Amendment's protections. *Id.* at 265. Second, the Icelandic Server was searched by Icelandic authorities, to whom, as Clark concedes (Def. Br. 19–20), the Fourth Amendment and its exclusionary rule do not apply. Third, as Clark apparently concedes (Def. Br. 20), any seizure and search of the Icelandic Server by foreign authorities was reasonable. The foreign search doctrine squarely controverts Clark's baseless suggestion that a warrant is required to review a copy of lawfully obtained and previously imaged foreign evidence once it crosses the United States border. Fourth, even if Clark's novel argument were accepted, the exclusionary rule would not apply because the law enforcement officers acted in good faith based on then-existing binding law.

A. The FBI's Review of the Icelandic Server Did Not Violate the Fourth Amendment

1. <u>As A Canadian Citizen Then in Thailand Who Had No Voluntary, Substantial Connection to This Country, Clark Is Not Among "The People" Who May Assert the Fourth Amendment's Protections to Challenge Investigative Steps Taken in Iceland</u>

In *United States v. Verdugo-Urquidez*, a plurality of the Supreme Court held that a non-resident alien, with "no voluntary attachment to the United States," could not invoke the protections of the Fourth Amendment to suppress evidence obtained through a warrantless search of his property abroad. 494 U.S. at 274–75. The Court reasoned that the Fourth Amendment did not apply to a nonresident foreign national in these circumstances because "'the people' protected by the Fourth Amendment . . . refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that

community." *Id.* at 265. Thus, even the fact that the nonresident alien had been arrested, and involuntarily brought into the United States, days before his house was searched in Mexico did not establish the sort of sufficient voluntary ties to the United States that would extend the Fourth Amendment's protections to him. *Id.* Accordingly, the plurality concluded, "[a]t the time of the search, [defendant] was a citizen and resident of Mexico with no voluntary attachment to the United States, and the place searched was located in Mexico. Under these circumstances, the Fourth Amendment has no application." *Id.* at 274–75. In all, seven Justices of the Supreme Court in *Verdugo-Urquidez* "endorsed the view that U.S. courts are not empowered to issue warrants for foreign searches." *See In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 157, 169 (2d Cir. 2008) ("*In re Terrorist Bombings*").

The Second Circuit and district courts in this Circuit have adhered to these holdings. *See, e.g.*, *id.* at 174 (stating that, under *Verdugo-Urquidez*, "the Fourth Amendment affords no protection to aliens searched by U.S. officials outside of our borders"); *United States v. Mustafa*, 753 F. App'x 22, 43–44 (2d Cir. 2018) (summary order), *cert. denied*, 140 S. Ct. 274 (2019) (citing *Verdugo-Urquidez* for the proposition that a "foreign national cannot raise Fourth Amendment challenge to searches conducted abroad"); *United States v. Coke*, No. 07 Cr. 971 (RPP), 2011 WL 3738969, at *4 (S.D.N.Y. Aug. 22, 2011) (holding that foreign national defendant had no Fourth Amendment basis to suppress foreign wiretaps provided to U.S. authorities by Jamaican authorities because "where a defendant is not a United States citizen, and has no substantial, voluntary attachment to the United States, and the search at issue occurs abroad, the Fourth Amendment has no application.") (internal quotation marks omitted); *United States v. Gasperini*, No. 16 Cr. 441, 2017 WL 3038227, at *3 (E.D.N.Y. July 17, 2017), *aff'd*, 894 F.3d 482 (2d Cir. 2018) ("Defendant . . . lacked any connection to the United States prior to his extradition into this country . . . . As

such, he cannot claim that searches of his data stored outside the U.S. violated his Fourth Amendment rights."); *United States v. Defreitas*, 701 F. Supp. 2d 297, 304 (E.D.N.Y. 2010) ("Kadir is not a U.S. citizen, and has no voluntary connections to the United States. It is well settled that the Fourth Amendment is inapplicable to persons so situated, who are searched outside of the country. Thus, with respect to the searches and seizures conducted in Trinidad and Tobago and Guyana, an exclusionary remedy is unwarranted.") (citations omitted); *accord United States v. Loera*, 333 F. Supp. 3d 172, 181–82 (E.D.N.Y. 2018).

United States v. Loera, the recent prosecution of Sinaloa drug cartel leader "El Chapo," is particularly instructive on this issue under analogous circumstances. Acting in response to an MLAT request submitted by the FBI, Dutch authorities executed search warrants on servers located in the Netherlands that ran the defendant's encrypted communications network, and provided the FBI with copies of their contents. *Loera*, 333 F. Supp. 3d at 180–81. The defendant, a Mexican national, moved to suppress evidence from Dutch servers as a violation of his Fourth Amendment rights. *Id.* at 180. The district court rejected the motion, finding that the searches occurred in the Netherlands and that defendant lacked sufficient voluntary ties to the United States to entitle him to Fourth Amendment protections:

> [T]he searches occurred in the Netherlands, and defendant was a citizen and resident of Mexico at that time. As a result, defendant can only invoke the Fourth Amendment if he has established substantial voluntary connections to the United States. Defendant argues that, because the Government claims that he and the Sinaloa Cartel directed a large-scale narcotics trafficking operation into the United States and sold millions of dollars of drugs here, the Government has alleged sufficient connections to afford him Fourth Amendment protections. But defendant – not the Government – bears the burden of establishing that his Fourth Amendment rights were violated. Because he has not provided any facts other than the Government's theory of the case, defendant has not met his burden to show substantial connections with this country that might otherwise entitle him to Fourth Amendment protections. Even if defendant could establish a connection to this country through the Government's charges against him, defendant's conduct does not constitute the type of connections that the Supreme Court envisioned when it

> spoke of the community of people covered by the Fourth Amendment. Rather, his alleged connections are purely criminal and do not entitle him to protection. Ultimately, defendant's story parallels that of the respondent's in *Verdugo-Urquidez*, and the Supreme Court was clear that the Fourth Amendment did not apply in that instance.

Id. at 182 (internal citations omitted).

Clark, a Canadian citizen, lived abroad prior to and during the time of the search, and was extradited to the United States approximately five years after the search took place in Iceland. Like the defendant in *Loera*, Clark's ties to this country are solely criminal in nature. On those undisputed facts, he has plainly "not met his burden to show substantial connections with this country that might otherwise entitle him to Fourth Amendment protections." *Loera*, 333 F. Supp. 3d at 180. If anything, Clark's claim is even weaker than the claim made by the defendant in *Verdugo-Urquidez* who was at least *in* the United States (in prison, in California) while U.S. law enforcement conducted a search of his homes in Mexico. Clark, by contrast, had literally no tie to the United States whatsoever. Thus, like the defendant in *Verdugo-Urquidez*, and the other authority recited above, Clark cannot invoke the Fourth Amendment as to the search of foreign property in which he claims to have an interest.

2. The Fourth Amendment and the Exclusionary Rule Do Not Apply to Searches of Foreign Property by Foreign Law Enforcement

In any case, regardless of Clark's ties to the United States or lack thereof, the law has long been clear that the Fourth Amendment and the exclusionary rule do not extend to searches conducted outside the United States by foreign law enforcement authorities. *See, e.g.*, *United States v. Lee*, 723 F.3d 134, 139 (2d Cir. 2013) ("[T]he Fourth Amendment's exclusionary rule, which requires that evidence seized in violation of the Fourth Amendment must be suppressed, generally does not apply to evidence obtained by searches abroad conducted by foreign officials."); *United States v. Busic*, 592 F.2d 13, 23 (2d Cir. 1978) ("[T]he Fourth Amendment and its

exclusionary rule do not apply to the law enforcement activities of foreign authorities acting in their own country."); *accord United States v. Vilar*, 729 F.3d 62 (2d Cir. 2013).

It is well established that "'information furnished [to] American officials by foreign police need not be excluded simply because the procedures followed in securing it did not fully comply with our nation's constitutional requirements.'" *United States v. Getto*, 729 F.3d 221, 227 n.7 (2d Cir. 2013) (quoting *United States v. Cotroni*, 527 F.2d 708, 711 (2d Cir. 1975)). The reason for this is that "[t]he exclusionary rule is intended to inculcate a respect for the Constitution in the police of our own nation. Since it has little if any deterrent effect upon foreign police, it is seldom used to bar their work product." *Cotroni*, 527 F.2d at 711. Searches by foreign law enforcement authorities implicate constitutional restrictions only in two narrowly limited circumstances: "(1) where the conduct of foreign law enforcement officials rendered them agents, or virtual agents, of United States law enforcement officials; or (2) where the cooperation between the United States and foreign law enforcement agents is designed to evade constitutional requirements applicable to American officials." *Getto*, 729 F.3d at 230. The defendant does not argue that either circumstance was present here or challenge the reasonableness of the foreign search. Nor could he. The Silk Road website hosted by the Icelandic Server was known to host a vast criminal enterprise. The Icelandic Server was imaged by Icelandic authorities, specifically, the RMP. RMP personnel obtained all legal process needed under Icelandic law to search the Icelandic Server and executed the imaging of the server themselves.

3. The FBI's Domestic Review of Evidence Lawfully Searched and Seized by Icelandic Authorities in Iceland Is Not a New Search to which the Warrant Clause Applies

Apparently recognizing the clear import of *Verdugo-Urquidez* and the foreign search doctrine, Clark does not contest the "imaging of the servers in Iceland." (Def. Br. 20). He instead attempts to end-run this wall of authority by arguing that the purported Fourth Amendment

violation happened later, in the United States, because that is where the FBI reviewed copies of the contents of the Icelandic Server received from Icelandic authorities. Clark neglects to offer any legal support for his specious argument that evidence lawfully seized and imaged abroad by foreign authorities triggers the Warrant Clause's requirements if FBI later obtains a copy of that evidence and chooses to review it in the United States. And for good reason. The defendant's proposed bifurcation between a lawful foreign search and seizure and a domestic review of the same evidence would effectively render the entirety of foreign search doctrine a dead letter.

Any seizure and search of the Icelandic Server occurred abroad, when Icelandic authorities seized the server and imaged its contents. Before analyzing the scope of the Fourth Amendment, the *Verdugo-Urquidez* Court "[thought] it significant to note" that Fourth Amendment violations are "fully accomplished" at the time of an unreasonable governmental intrusion. *Id.* at 264. Therefore, the Court observed, "[f]or the purposes of this case . . . if there were a constitutional violation, it occurred solely in Mexico." *Id.*; *see also In re Terrorist Bombings*, 552 F.3d at 199 ("Because a putative violation of the Fourth Amendment is 'fully accomplished' at the place and time of the alleged intrusion . . . a claimed violation occurring overseas entails an analysis of the extraterritorial application of the Fourth Amendment."). *Verdugo-Urquidez* and its progeny thus implicitly reject the baseless notion, advanced by Clark, that transporting the same evidence seized and searched abroad into the United States for the FBI's review triggers a new "search" in the United States and a corresponding warrant requirement.

Clark's argument has been advanced by at least one other defendant, unsuccessfully. In *United States v. Defreitas*, the defendant argued that he suffered a Fourth Amendment violation when physical drives seized from his foreign residence in Guyana were searched in the United States. 701 F. Supp. 2d 297, 306 & n.11 (E.D.N.Y. 2010). Unlike the digital contents of the

Icelandic Server, however, which were repeatedly accessed by Icelandic authorities in Iceland as part of their imaging and copying processes, the contents of the physical drives in *Defreitas* do not appear to have been accessed by law enforcement in Guyana before they arrived in the United States. Nonetheless, the court rejected the defendant's attempt to apply the Fourth Amendment to the domestic review of the drives, reasoning that it would be "incongruous to hold that *Verdugo-Urquidez* applied during the initial seizure in Guyana, and then became inapplicable *to the same evidence* once it was brought into this country." *Id.* (emphasis in original). Here, *a fortiori*, the relevant search and seizure occurred abroad when Icelandic authorities imaged the Icelandic Server in Iceland and provided the FBI copies of the evidence. *See Loera*, 333 F. Supp. 3d at 182 ("[T]he Dutch authorities conducted *searches* when they accessed and copied the contents of the Dutch servers pursuant to search warrants, and when they transferred those copies to the FBI.") (emphasis added). That the FBI chose to subsequently analyze that evidence in the United States has no bearing on where the search of the server occurred in the first place.

Finally, Clark remarkably argues that the Government "implicitly acknowledged" that it needed a warrant for the Iceland Server by obtaining warrants to search two servers in the United States. (Def. Br. 20). Clark ignores the obvious fact that the Government obtained those warrants because the servers were physically located *in the United States* when they were seized and searched and thus within purview of the Warrant Clause; the server in Iceland was not.

4. The Good Faith Exception to the Exclusionary Rule Applies Here

For the reasons stated above, the Fourth Amendment does not apply to Clark or to the search of the Icelandic Server, and there was no requirement to obtain a warrant for U.S. law enforcement to analyze a copy of the Icelandic Server provided to them by foreign authorities. Accordingly, there is no basis to suppress evidence from the Icelandic Server or any fruits from

the review of that server. However, even if the Warrant Clause were found to apply in the circumstances present here, the exclusionary rule would not apply because the law enforcement officers acted in good faith based on then-existing law.

Even if a Fourth Amendment violation were found, and there is none here, that does not necessarily mean that the exclusionary rule applies. *Herring v. United States*, 555 U.S. 135, 140 (2009). As the Supreme Court has observed, "exclusion has always been our last resort, not our first impulse." *Id.* (internal quotation marks omitted). The "[exclusionary] rule's sole purpose . . . is to deter future Fourth Amendment violations." *Id.* at 236–37. Thus, "when the police act with an objectively reasonable good-faith belief that their conduct is lawful or when their conduct involves only simple, isolated negligence, the deterrence rationale loses much of its force, and exclusion cannot pay its way[.]" *Id.* at 348 (internal citations and quotations omitted).

"The good-faith exception provides that 'searches conducted in objectively reasonable reliance on binding appellate precedent are not subject to the exclusionary rule.'" *United States v. Aguiar*, 737 F.3d 251, 259 (2d Cir. 2013) (quoting *Davis v. United States*, 564 U.S. 229, 232 (2011)). The deterrent effect of exclusion in such a case can only be to discourage the officer from "do[ing] his duty." *Davis*, 564 U.S. at 241. The exclusionary rule similarly does not apply when the police conduct a search in "objectively reasonable reliance" on a subsequently invalidated search warrant. *United States v. Leon*, 468 U.S. 897, 922 (1984). Although the burden is on the Government to establish good faith, "[s]earches pursuant to a warrant will rarely require any deep inquiry into reasonableness, for a warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search." *Id.* (citations and internal quotation marks omitted); *see also United States v. Rickard*, 534 F. App'x 35, 37 (2d Cir. 2013) (summary order) ("Most such searches will be upheld.").

At the time of the searches at issue in 2013, *Verdugo-Urquidez* had established that the Fourth Amendment did *not* apply to searches of foreign citizens' property conducted abroad, and *In re Terrorist Bombings* had established that the warrant requirement does not apply to searches abroad and that the government has a compelling interest in disrupting complex criminal organizations. *In re Terrorist Bombings*, 552 F.3d at 175–76. Thus, "law enforcement officials conformed their conduct to existing Supreme Court and Second Circuit law while conducting searches on the [foreign] servers. This counsels against application of the exclusionary rule, because its deterrent value simply would not be furthered in this case." *Loera*, 333 F. Supp. 3d at 183–84. Accordingly, applying the exclusionary rule to the Icelandic Server would not serve any deterrent purposes.

There is even less basis to exclude evidence obtained through the warrants issued subsequent to the review of the Icelandic Server (the "Subsequent Warrants"). When the affiant candidly informs the magistrate judge of all the relevant facts, including those that could be interpreted to undermine the validity of the warrant, the Second Circuit has found good faith reliance on the resulting warrant as long as such reliance is not unreasonable. *See United States v. Thomas*, 757 F.2d 1359, 1368 (2d Cir. 1985) (holding district court correctly denied suppression motion where DEA agent informed magistrate of a warrantless canine sniff test later determined to be unlawful and relied on magistrate's issuance of warrant); *see also United States v. DeProspero*, 472 F. App'x 42, 43–44 (2d Cir. 2012) (summary order) (applying good faith rule where the "application for the federal search warrant presented all the relevant facts to the federal magistrate judge, including the information" concerning portion of search that defendant argued was unlawful) (citing *Thomas*)).

The affidavits seeking the Subsequent Warrants truthfully explained that the FBI had located the server hosting the Silk Road website in a foreign country and obtained an image of the server's contents through an official request to that country. (*See, e.g.*, Tarbell Decl. Exs. E-G & L-O; Ulbricht Laptop Search Warrant Affidavit ¶ 9 ("[T]he FBI has located in a certain foreign country the server used to hold Silk Road's website . . . . Pursuant to a Mutual Legal Assistance Treaty request, an image of the Silk Road Web Server was made on or about July 23, 2013, and produced therafter to the FBI.")). None of the affidavits concealed how the FBI obtained the server, or suggested that the FBI reviewed it pursuant to a domestic search warrant after obtaining it from foreign law enforcement. The defendant does not argue that the issuing magistrates were knowingly misled in any way or issued facially deficient warrants so lacking in any indicia of probable cause that it was unreasonable to rely on them. *See United States v. Clark*, 638 F.3d 89, 100 (2d Cir. 2011).[11] Indeed, different magistrate judges in three different districts approved the affidavits at issue, including the nearly identical language they all contained concerning the acquisition of a copy of the Icelandic Server from abroad and its inclusion in the mix of probable cause. Deference to their determinations is thus especially warranted. *See United States v. Carpenter*, 341 F.3d 666, 670 (8th Cir. 2003) (fact that multiple judges found application to establish probable cause underscores deference owed by reviewing court).

[11] In Ross Ulbricht's motion to suppress, Ulbricht argued that the magistrate judges who received the warrant applications discussing the review of the Icelandic Server failed appropriately to inquire into how the preliminary investigation was conducted. The Court denied the motion based on Ulbricht's threshold failure to demonstrate a privacy interest in the server, but observed in dicta that it would find no deficiency in the subsequent warrants, finding it "apparent from the face of the affidavit" of one of the challenged warrants that "the application was carefully reviewed and probable cause established." *United States v. Ulbricht*, 14 Cr. 68 (KBF), Dkt. 89 (Opinion and Order) at 23 n.8.

Because nothing here suggests that the searching agents should have known that, despite being authorized by the Subsequent Warrants, their search (purportedly) ran afoul of the law, the motion should be denied as to the Subsequent Warrants as well.[12]

B. Clark Also Lacks Standing Under the Fourth Amendment

1. Applicable Law

"A defendant seeking to suppress the fruits of a search by reason of a violation of the Fourth Amendment must show that he had a 'legitimate expectation of privacy' in the place searched." *United States v. Hamilton*, 538 F.3d 162, 167 (2d Cir. 2008) (quoting *Rakas v. Illinois*, 439 U.S. 128 (1978)). "This inquiry involves two distinct questions: first, whether the individual had a subjective expectation of privacy; and second, whether that expectation of privacy is one that society accepts as reasonable." *Id.* It is the defendant's burden to make these showings. *Rawlings v. Kentucky*, 448 U.S. 98, 104 (1980).

The Fourth Amendment applies differently for commercial premises than it does for a residence. *See New York v. Burger*, 482 U.S. 691, 699 (1987). While under certain circumstances an employee may have a reasonable expectation of privacy in his workplace and may have standing

[12] Even if a Fourth Amendment violation were found and the exclusionary rule were held to apply to the Icelandic Server, and it should not, "the mere inclusion of tainted evidence in an affidavit does not, by itself, taint the warrant or the evidence seized pursuant to the warrant[.]" *United States v. Reilly*, 76 F.3d 1271, 1282 n.2 (2d Cir. 1996). Rather, the Court must "excise the tainted evidence and determine whether the remaining, untainted evidence would provide a neutral magistrate with probable cause to issue a warrant." *Id.* (quoting *United States v. Vasey*, 834 F.2d 782, 788 (9th Cir. 1987) (internal quotations and alternations omitted)). Aside from tersely noting that the Government "recited and relied on information it got from examining the contents of the [Silk Road] servers" in certain warrants (Def. Br. 21), the defendant did not parse the other indicia of probable cause as to those warrants. Should the Court rule for Clark on all Fourth Amendment questions, a second round of briefing would be needed to determine, warrant-by-warrant, precisely what portion of probable cause was tainted, and what untainted residue remains.

to challenge a search of its premises, such an expectation "is different from, and indeed less than, a similar expectation in an individual's home." *Id.* at 700.[13] An adequate showing requires the employee to demonstrate (1) a "possessory or proprietary interest in the area searched," and (2) a "sufficient nexus between the area searched and his own work space." *United States v. Chuang*, 897 F.2d 646, 649 (2d Cir. 1990). Unlike the nearly absolute protection of a residence, the "great variety of work environments" requires analysis of reasonable expectations "on a case-by-case basis." *O'Connor v. Ortega*, 480 U.S. 709, 718 (1987). Indeed, certain industries "have such a history of government oversight that no reasonable expectation of privacy . . . could exist." *Marshall v. Barlow's, Inc.*, 436 U.S. 307, 313 (1978); *see also O'Connor*, 480 U.S. at 718 ("[S]ome government offices may be so open to fellow employees or the public that no expectation of privacy is reasonable.").

Generally, courts tend to find that a defendant (in a corporate setting) does have standing when the area searched is set aside for the defendant's *exclusive* use, such as an individual office. *See, e.g., Leventhal v. Knapek*, 266 F.3d 64, 73 (2d Cir. 2001) (employee had reasonable expectation of privacy in the contents of *his* office computer where he had a *private* office and had *exclusive* use of the desk, filing cabinet, and computer in his office); *United States v. Taketa*, 923 F.2d 665 (9th Cir. 1991) (corporate vice president had standing to challenge search of his own office). Courts also give weight to the fact that a defendant was, for instance, the *only person* with a key to a corporate premises. *See, e.g., United States v. Chaves*, 169 F.3d 687, 691 (11th Cir. 1999) (defendant had standing to challenge search of warehouse where he possessed the *only key*

[13] Indeed, aside from Fourth Amendment protection against overbroad subpoenas, "neither the officers of a corporation, the shareholders . . . nor the corporation itself has any other Fourth Amendment interest in corporate records." *United States v. Lartey*, 716 F.2d 955, 961 (2d Cir. 1983) (citations omitted).

to warehouse and stored personal and business papers there). The greater the degree of exclusivity and control over a work area, and the more time a defendant spends there, the more likely standing is to be found. By contrast, the less private a work area—and the less control a defendant has over that work area—the less likely standing is to be found. *See, e.g.*, *United States v. Filippi*, No. 12 Cr. 604 (RA), 2013 WL 208919, at *3–5 (S.D.N.Y. Jan. 16, 2013) (denying suppression motion where defendant "claims no ownership interest in the Warehouse and makes no representation that he exercised exclusive use or control over any specific area"); *Martinez v. Nygaard*, 831 F.2d 822 (9th Cir. 1987) (factory workers could not challenge search of common area used by 75 people).

These standing principles have repeatedly been applied in cases involving corporate executives. In *United States v. Chuang*, the defendant served as the chairman, president, and CEO of Golden Pacific National Bank, and owned with his family nearly half of the shares of the bank and "exercised significant operational control over the bank and all of its premises." 897 F.2d 646, 650 (2d Cir. 1990). The district court denied Chuang's motion to suppress the fruits of the search of the bank and the resulting seizure of electronic materials, due to lack of standing. On appeal, Chuang argued that, as a corporate officer, he had a sufficient expectation of privacy in the bank premises to challenge the search. *Id.* The Second Circuit affirmed, noting that "the bulk of the bank documents" were seized from the office of another bank officer, and finding that Chuang had "failed to demonstrate a sufficient nexus between the areas from which the documents were obtained and his own office." *Id.*[14] Other courts' decisions are in accord.[15]

[14] The Second Circuit also found, as another reason to deny suppression, that Chuang failed to demonstrate a reasonable expectation of privacy because he worked in a "closely regulated industr[y]" and, as a result, Chuang "knew that bank documents, whether kept in his office or another office, were subject to periodic examination." *Chuang*, 897 F.2d at 650.

[15] *See, e.g.*, *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 694, 698 (9th Cir. 2009) (denying challenge of business owners to search of corporation's premises because mere

In three recent cases, corporate executives or supervisors have moved to suppress evidence seized from corporate servers, and in each case, courts have found a lack of standing. *See, e.g.*, *United States v. Nagle*, 803 F.3d 167, 178–79 (3d Cir. 2015) (defendant—the co-owner of a company—lacked standing to challenge search of (1) computers seized from other employees' offices, and (2) corporate servers, even as to his own emails on those servers); *United States v. Mendlowitz*, 17 Cr. 248 (VSB), 2019 WL 1017533, at *5 (S.D.N.Y. Mar. 2, 2019) (defendant—the co-owner, president, and CEO of the company—lacked a reasonable expectation of privacy in the corporate servers or the computers seized from locations other than his own office); *United States v. Costin*, 05 Cr. 38 (JCH), 2006 WL 2522377, at *6 (D. Conn. July 31, 2006) (defendant—the senior supervisor at the company—lacked standing to challenge search of company's servers, as he failed to show control or possession of data stored on company's computers, aside from that located on his desk; but he did have standing as to two physical locations where he worked and stored personal files).

2. Application

The foregoing principles compel the conclusion that Clark has failed to establish standing in the Icelandic Server. Clark has not come close to establishing standing even if one accepts, *arguendo*, Clark's self-serving, uncorroborated claims in his Declaration that he was a part-owner

---

ownership and management is insufficient to challenge search, but finding that defendants could show a legitimate expectation of privacy in corporation's property if they "show[ed] some personal connection to the places searched and the materials seized" and "took precautions on [their] own behalf to secure the place searched or things seized from any interference without [their] authorization"); *Williams v. Kunze*, 806 F.2d 594, 594, 599–604 (5th Cir. 1986) (concluding that sole shareholder of corporation lacked standing where "the vast majority of documents seized . . . were corporate records" rather than personal files and defendant "had no reasonable expectation of privacy in corporate records maintained in a common file room"); *United States v. Britt*, 508 F.2d 1052 (5th Cir. 1975) (corporate president has standing to challenge search of corporate records in his office but not corporate records in storage area).

of Silk Road—which directly contradict his prior testimony under oath in Thailand that he had no involvement in the website whatsoever.[16]

As a preliminary matter, the comprehensive record developed through the Ulbricht trial contains zero support for Clark's claim that he was a part-owner. That record makes the following points clear, among various others:

1. Ulbricht conceived of Silk Road, launched it in early 2011, and oversaw all aspects of its operation until his arrest on October 1, 2013.

2. Ulbricht leased, owned, controlled, and paid for every Silk Road server. In fact, the Ulbricht Laptop contained a spreadsheet (entitled "Servers.ods") with detailed information about every server he used for Silk Road, including the location of the server, the type of server, the IP address, the email address and alias used to register the server, his password, when the server expires, and what he uses that server for (*e.g.*, marketplace, forum, backup, active wallets, "tor relay," etc.). This "Servers" spreadsheet contained notes about more than 40 "active" servers and more than a dozen "retired" servers.

3. At the time of his arrest, Ulbricht was accessing the Silk Road "Mastermind" webpage, the top-level administrative page for Silk Road. Forensic analysis of the Silk Road server showed that the "Mastermind" webpage could only be accessed using "Dread Pirate Roberts"'s account on the server, and could not be accessed by any of the other Silk Road staff employees.

4. The Ulbricht Laptop contained a folder with his employees' identifications, including Clark's Canadian Passport. Ulbricht therefore knew "VJ"/"cimon"'s true identity. The Ulbricht-Clark chats contain no evidence that Clark knew Ulbricht's identity. (Even now, Clark refers to Ulbricht as "DPR" in his Declaration.)

5. Ulbricht paid Clark in Bitcoin repeatedly, including payments of approximately: (1) $93,150 on or about November 16, 2012; (2) $50,000 on or about May 7, 2013; and (3) $57,000 on or about July 3, 2013.

6. The Ulbricht Laptop had a detailed accounting spreadsheet including repeated entries for "server rent," "payroll," and "commissions," as well as sporadic

[16] Because even his self-serving, uncorroborated claims are insufficient to establish standing, the Government does not view it as necessary, in this brief, to explain comprehensively why several of the key allegations in Clark's Declaration are contradicted by the record established through Ulbricht trial. However, the Government supplies certain examples above and reserves its right to file such a brief, in the event it is necessary to resolve the instant motions.

entries for "bounties," "420 grand prize," and "pay off hacker." There is never an entry that suggests that anyone else received a portion of Silk Road profits/commissions.

7. Ulbricht told the Silk Road community, "Whether you like it or not, I am the captain of this ship. You are here voluntarily and if you don't like the rules of the game, or you don't trust your captain, you can get off the boat."

8. As Ulbricht wrote in his journal, Variety Jones (*i.e.*, Clark) "convinced me of a server configuration paradigm that gave me the confidence to be *the sole server administrator* and not work with someone else at all." (Emphasis added).

9. Clark deferred to Ulbricht for final decisions. For instance, as noted above, Clark recommended that Ulbricht commission a murder-for-hire because an individual had stolen from Silk Road. After Clark made this recommendation, Ulbricht said he wanted to think about it. Shortly thereafter, the following chat occurred:

> Cimon: So, you've had your time to think. You're sitting in the big chair, and you need to make a decision. Now, really, things could move fast in the future.
>
> DPR: I would have no problem wasting this guy
>
> Cimon: Well ok then, I'll take care of it.

10. In the months that followed, Ulbricht commissioned four more murders-for-hire. Ulbricht did not even tell Clark before doing so.

Turning to the claims in Clark's Declaration, Clark alleges, among other things, that he "provided advice [to DPR] on the technical aspects of running the site," "helped him hire and manage an experienced programmer," "assisted DPR in developing computer code and maintaining Silk Road's technical infrastructure," "became *de facto* head of marketing," "agreed to take an ownership interest in the business," and was "a part-owner of Silk Road" from February 2013 until the site was taken down in October 2013. (Clark Decl. ¶¶ 7, 9, 13, 14).

The lengthy line of case law discussed above makes plain that Clark's allegations are well short of establishing standing in the Icelandic Server. Clark has not alleged, for instance, that he

owned, leased, or controlled the Icelandic Server. He has not alleged that he had special access to the Icelandic Server. He has not alleged that he was an administrator of the Icelandic Server. He has not alleged that he could see other individuals' communications on the Icelandic Server. He has not alleged that his own communications on the Icelandic Server could not be monitored by Ulbricht or any other individuals with access to the Icelandic Server. He has not alleged that he knew the user name, password, alias, or even the IP address of the Icelandic Server. He has not alleged that he was ever at the physical location that hosted the Icelandic Server. He has not alleged that he ever communicated with the company that hosted the Icelandic Server. He has not alleged that he has any link to the "Servers.ods" file on the Ulbricht Laptop. (In fact, he has not even alleged what percent owner he purportedly was, or when exactly he became a part-owner.) He has not alleged that he knew the Bitcoin "private keys," which is where Silk Road's commissions went. He has not alleged that he was entitled to, or received, a portion of Silk Road's profits. He has not alleged that he even knew who his purported co-owner was.

As the Second Circuit has made clear, the "question whether a corporate officer has a reasonable expectation of privacy to challenge a search of business premises focuses principally" on two questions: (1) "whether he has made a sufficient showing of a possessory or proprietary interest in the area searched"; and (2) whether he can "demonstrate a sufficient nexus between the area searched and his own work space." *Chuang*, 897 F.2d at 649. Clark cannot make either showing. He has no possessory or proprietary interest in the Icelandic Server, nor has he alleged any. He did not own, lease, control, administer, or pay for that server. Nor can he show the required "nexus" between his work space (his computer in Thailand) and the Icelandic Server. The fact that he was a user of Silk Road, and used the website to sell marijuana seeds, does not differentiate him from the more than 100,000 Silk Road users. *See United States v. Watson*, 404

F.3d 163, 166 (2d Cir. 2005) (affirming denial of suppression motion without a hearing, because the claims made in a declaration—that the defendant was among those who "utilized" the location searched—"d[id] not come close to showing that defendant owned the premises or that he occupied them and had dominion and control over them by leave of the owner") (citation and internal quotation marks omitted).

Clark's standing claims are meaningfully weaker than the claims raised in a host of the cases discussed above, including *Chuang* (defendant was chairman, president, CEO, and part-owner), *Williams* (sole shareholder), *Mendlowitz* (co-owner, president, and CEO), and *Nagle* (co-owner). In those cases, the defendants possessed far greater control over their respective entities than did Clark; nonetheless, four different courts rejected all four of those defendants' claims. *See Chuang*, 897 F.2d at 650 (the defendant—the chairman, president, CEO, part-owner, and person who "exercised significant operational control over the bank and all of its premises"—lacked standing because "the bulk of the bank documents" were seized from another bank officer's office, and the defendant "failed to demonstrate a sufficient nexus between the areas from which the documents were obtained and his own office"); *Williams*, 806 F.2d at 594, 599–604 (sole shareholder of corporation lacked standing where "the vast majority of documents seized . . . were corporate records" rather than personal files and defendant "had no reasonable expectation of privacy in corporate records maintained in a common file room"); *Mendlowitz*, 2019 WL 1017533, at *5 (co-owner, president, and CEO of the company did not have reasonable expectation of privacy in the corporate servers or the desktop computers seized from locations other than his own office); *Nagle*, 803 F.3d at 178–79 (co-owner of company lacked standing both as to the computers seized from the offices of other employees, and as to corporate servers, because he had no expectation of privacy in the offices of others; and even as to his own emails on the corporate

servers, he had failed to show a subjective expectation of privacy); *see also, e.g.*, *Britt*, 508 F.2d at 1055–56 (although defendant was sole shareholder and president of corporation whose property was searched, he lacked standing where he did not personally use the space searched).

There is an additional reason that Clark could not have had a reasonable expectation of privacy: the materials on the Icelandic Server are *business records*, including transactional data for sales made on Silk Road. (The Government routinely subpoenas these sorts of records—at least in the case of legitimate businesses.) The overwhelming majority of these transactions on Silk Road did not involve Clark; and the overwhelming majority of communications on Silk Road did not involve Clark. The Government is aware of *nothing* on the Icelandic Server from Clark's private space or home office; of course, that would be completely at odds with the essence of Silk Road—a criminal marketplace involving users with aliases, not a filing cabinet for one's personal items. *See Williams*, 806 F.2d at 594, 599–604 (sole shareholder lacked standing where "vast majority of documents seized . . . were corporate records" rather than personal files and defendant lacked reasonable expectation of privacy in corporate records maintained in a common room). These observations are particularly relevant here, because the Government expects that, at trial, the primary evidence from the Icelandic Server will be transactional data to prove the conspiracy's scope. (The primary source of *Clark's* communications are chats on the Ulbricht Laptop.)

And even as to Clark's very minimal communications through Silk Road servers, Clark *knew* that these were not private—and thus he could not have had a reasonable expectation of privacy in them. For instance, when Clark was advocating for the murder-for-hire discussed above, he told Ulbricht that the person who had stolen from Silk Road was a customer service representative who could read other people's private messages on Silk Road: "Dude, he was a

CSR [customer service representative] that could read PMs [private messages], reset passwords, mebbe harvest addys [addresses] while emptying accounts, etc., etc."[17]

* * *

In sum, this is not a close call. Under the Fourth Amendment, the standing inquiry ultimately turns on whether "the disputed search and seizure has infringed an *interest of the defendant* which the Fourth Amendment was *designed* to protect." *Rakas*, 439 U.S. at 140 (emphases added). It is emphatically clear that the Fourth Amendment was not designed to protect a Canadian citizen residing in Thailand from complaining about the search of an Icelandic server he did not own, lease, control, administer, or pay for.[18]

C. Clark's Packet-Sniffing Argument, Which Also Seeks to Invoke the Fourth Amendment, Fails

Clark states that two federal agents discovered the IP address of a Silk Road server by making entries into the Silk Road login page and examining the packets of data that were returned (so-called "packet-sniffing"). Clark argues that packet sniffing is a search protected by the Fourth

[17] The Second Circuit has explained that those who email and communicate over the Internet generally lose a legitimate expectation of privacy in such communications that have already reached their recipient. *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) (citing *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001) ("Users would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting. They would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient; at this moment, the e-mailer would be analogous to a letter-writer, whose expectation of privacy ordinarily terminates upon delivery of the letter.") (internal citations and quotation marks omitted)). The basis for any expectation of privacy is even weaker when the individual knows that *third parties* have access to his online communications, as well.

[18] It is also worth noting that the Icelandic Server hosted a publicly available website. In the highly unlikely event that the Court disagrees with the foregoing analysis, the answer would not be that Clark has standing as to the full contents of the Icelandic Server. It would be necessary to differentiate between various types of information on the Icelandic Server, some of which (for instance) was plainly available to the public, while other aspects (for instance) were accessible only to Ulbricht. *See, e.g.*, *United States v. Meregildo*, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012) (noting that web content accessible to the public is not protected by the Fourth Amendment and can be viewed by law enforcement agents without a warrant).

Amendment and that a warrant was required. (Def. Br. 22–33). Clark's argument about "packet sniffing" is baseless; there are at least four fundamental flaws with his argument.

First, Clark's argument is explicitly foreclosed by binding Second Circuit authority. In the *Ulbricht* appeal, the Second Circuit held that:

> Like telephone companies, Internet service providers require that identifying information be disclosed in order to make communication among electronic devices possible. In light of the *Smith* rule, no reasonable person could maintain a privacy interest in that sort of information. We therefore join the other circuits that have considered this narrow question and hold that collecting IP address information devoid of content is constitutionally indistinguishable from the use of a pen register.

United States v. Ulbricht, 858 F.3d 71, 97 (2d Cir. 2017) (citing decisions by the Third, Fourth, Sixth, Eighth, and Ninth Circuits), *cert. denied*, 138 S. Ct. 2708 (2018).

Clark cites zero cases for the proposition that packet sniffing even rises to the level of a search, nor has the Government found any. This is unsurprising. A website's IP address is non-content information that is extremely limited in scope; it reveals no information whatsoever about any particular person operating or accessing the website or their location; and the website's founder had chosen to create a massive marketplace and to make that website publicly available. These considerations are the touchstones of the Fourth Amendment analysis. This case is a therefore far cry from the cases relied on by Clark, because those cases all involve significant personal privacy interests in the United States—either an individual's location (*Carpenter*, *Lambis*) or the activity within an individual's home (*Kyllo*). Those types of details—when a specific person goes to particular places, or what a specific person does within the sanctity of his own home—are deeply personal. A website's IP address is not; indeed, it involves no personal privacy interests at all. Rather, an IP address is simply a website identifier that is as sterile, impersonal, and limited as information can be: 6 to 10 digits. That's it. (Thus, while the IP address for the Icelandic Server led to Iceland, Ulbricht was halfway across the globe in San Francisco.)

Clark strains to draw support from *Carpenter v. United States*, 138 S. Ct. 2206 (2018). But *Carpenter* did not deal with packet sniffing, did not overrule the Second Circuit's opinion in *Ulbricht*, and is inapposite here. In *Carpenter*, the Supreme Court held that "an individual maintains a legitimate expectation of privacy in the *record of his physical movements* as captured through CSLI [cellsite location information]." *Id.* at 2217 (emphasis added). The *Carpenter* Court explained that time-stamped CSLI "provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations." *Id.* (citations and internal quotation marks omitted). The Court elaborated, "[a] cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Id.* at 2218. And such location information is saved by wireless carriers for up to five years, and is captured for everyone; "[o]nly the few without cell phones could escape this tireless and absolute surveillance." *Id.* In explaining why the third-party doctrine did not apply to CSLI, the Court noted, "[t]here is a world of difference between the *limited types of personal information* addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today." *Id.* at 2219 (emphasis added). The Court therefore ruled that a warrant was generally needed to obtain CSLI, given "the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection." *Id.* at 2223. None of these considerations applies to the extremely limited class of information obtained here—a series of sterile digits in Iceland, untethered to any person (and certainly not Clark), and revealing no information whatsoever about a person's movements, activities, or associations.

Clark's argument fails for at least three more reasons discussed in more detail above. First, even assuming *arguendo* that packet sniffing is a search, under these facts, it would be a foreign search outside the reach of the Fourth Amendment. Second, as a Canadian citizen then in Thailand, Clark has no standing to object to agents' review of Icelandic IP address information. And third, even if the Court disagrees with the foregoing, the good-faith exception plainly applies, especially given that the Second Circuit explicitly approved of this investigative technique in *Ulbricht*, a 2017 decision, based on then-controlling precedent. For all of these reasons, Clark's packet-sniffing arguments fail.

IV. CLARK'S THAILAND-RELATED MOTIONS ARE MERITLESS

Clark's Thailand-related motions can be divided into two buckets—his post-arrest statements and devices seized from him in Thailand. His motions to suppress his post-arrest statements in Thailand should be denied for two independent reasons: waiver and compliance with *Miranda*. His motions to suppress the contents of his devices should be denied for several reasons, including that it was eminently reasonable for foreign law enforcement officers to seize the electronic devices of a defendant charged with cyber crimes in connection with his arrest—especially where (as here) those devices were not searched before a judicially authorized warrant was obtained.

A. Clark Has Offered No Basis to Suppress His Post-Arrest Statements, Nor is There Any

As noted above, Clark made four different post-arrest statements in Thailand—two were oral statements, and two were written statements. Clark made all four statements while he was in Thai custody, but only the two oral statements were made in response to questioning. In these statements, Clark expressed interest in immunity; he conveyed significant technical expertise

involving Tor; and he repeatedly stated that he went by "Mongoose"—the same (highly unusual) name that he indicated he sometimes went by, in a chat with Ulbricht.

As a preliminary matter, Clark offers literally no basis at all for suppressing any, let alone all, of his post-arrest statements. He has simply moved to suppress each (*see* Dkt. 32 (Motion Statement), but entirely failed to explain the legal basis. In this situation, waiver applies. A party's failure to address an issue in its principal brief typically "constitutes waiver." *Gross v. Rell*, 585 F.3d 72, 95 (2d Cir. 2009) (citing *Zhang v. Gonzales*, 426 F.3d 540, 541 n.1 (2d Cir. 2005)). The Government cannot meaningfully respond when there are no reasons given, no citations offered, no bases supplied. Clark's motions to suppress his four post-arrest statements in Thailand should be denied on this ground alone.

When a statement or confession is obtained through interrogation of a defendant who is in custody, the Government must demonstrate that the defendant was informed of, and validly waived, his Fifth Amendment rights under *Miranda v. Arizona*, 384 U.S. 436 (1966). To prove a valid waiver of *Miranda* rights, the Government must show, by a preponderance of the evidence, that the defendant relinquished his rights voluntarily and that the defendant had a full awareness of the rights being waived and the consequences of waiving those rights. *See Colorado v. Connelly*, 479 U.S. 157, 167–69 (1986); *United States v. Jaswal*, 47 F.3d 539, 542 (2d Cir. 1995) (per curiam). The defendant need not "know and understand every possible consequence of a waiver of the Fifth Amendment privilege." *Colorado v. Spring*, 479 U.S. 564, 574 (1987). Rather, the accused need only be aware that his statements may be used against him in future prosecution, and that "he may choose not to talk to law enforcement officers, to talk only with counsel present, or to discontinue talking at any time." *Id.*

A related but distinct requirement is that a defendant's statement must be voluntary. A statement is not voluntary within the meaning of the Fifth Amendment if it is obtained by "'techniques and methods offensive to due process' or other circumstances in which the suspect clearly had no opportunity to exercise 'a free and unconstrained will.'" *Oregon v. Elstad*, 470 U.S. 298, 304 (1985) (quoting *Haynes v. Washington*, 373 U.S. 503, 514–15 (1963)). "No single criterion controls whether an accused's confession is voluntary: whether a confession was obtained by coercion is determined after a careful evaluation of the totality of the surrounding circumstances." *Green v. Scully*, 850 F.2d 894, 901 (2d Cir. 1988). The critical issue relevant to voluntariness looks to whether the defendant's will was "overborne" by the conduct of law enforcement officers such that his statements cannot be deemed to be the "product of a rational intellect and a free will." *Lynumm v. Illinois*, 372 U.S. 528, 534 (1963) (internal quotation marks omitted). "In applying the totality of the circumstances test, those factors that a court should consider to determine whether an accused's confession is voluntary center around three sets of circumstances: (1) the characteristics of the accused, (2) the conditions of interrogation, and (3) the conduct of law enforcement officials." *Green*, 850 F.2d at 901–02. The age of the accused, education level, intelligence, advice regarding constitutional rights, length of detention, repeated and prolonged questioning, and the use of physical punishment are some of the criteria that courts consider when further evaluating the totality of the circumstances. *Schneckloth v. Bustamonte*, 412 U.S. 218, 226 (1973). Compliance with *Miranda*, although not dispositive, is a significant factor weighing in favor of a finding of voluntariness, and "[i]n general, a suspect who reads, acknowledges, and signs an 'advice of rights' form before making a statement has knowingly and voluntarily waived *Miranda* rights." *United States v. Taylor*, 745 F.3d 15, 23 (2d Cir. 2014); *see also Berkemer v. McCarty*, 468 U.S. 420, 433 n.20 (1984).

The foregoing summarizes the familiar *Miranda* principles in a mine-run domestic case; "where *Miranda* has been applied to overseas interrogations by U.S. agents, it has been so applied in a flexible fashion to accommodate the exigencies of local conditions." *In re Terrorist Bombings*, 552 F.3d at 205. The Second Circuit has applied "[t]his context-specific approach." *Id.*

Clark has not even tried to argue any violation of these familiar principles, nor could he. In connection with both of his in-custody interviews with HSI Special Agent Joseph, Clark was advised of his *Miranda* rights orally and in writing. In both instances, Clark signed the advice-of-rights form, confirming his understanding of his rights. (*See* Exs. A and B). As for his written statements, these were not in response to questioning at all. Indeed, his written statements were the voluntary, deliberate, calculated words of a man who (by his own admission) sought immunity. There is no basis to suppress any of these statements.[19]

B. There Is No Basis to Suppress the Contents of Clark's Devices Seized in Thailand

Clark next seeks to suppress the contents of electronic devices seized from his home. He alleges that Thai officers beat him with sticks to induce him to sign a form consenting to the seizure of his devices. The Government is not aware of any information corroborating the defendant's self-serving claim. Clark's brief—filed nearly four years after the alleged events in question—was the first time that he mentioned these allegations to the Government, despite the fact that he made four separate post-arrest statements in Thailand over several months. In any event, Clark conflates two issues. The Government does not need the consent form. The Government is not relying on that form for its authority to search the devices, and does not intend to introduce the consent form in its case-in-chief. As for the devices, it was entirely reasonable (and unsurprising)

[19] Clark's final post-arrest statement occurred at the 500 Pearl Street courthouse in June 2018, on the day that he was extradited to the United States. The Government has no intention of using, in its case-in-chief, Clark's statement to FBI agents that day.

for the Royal Thai Police—aware that Clark was charged with sophisticated computer crimes—to seize Clark's computers and electronic devices.

1. Factual Background

By way of background, in or around April 2015, the United States submitted a request to the Kingdom of Thailand to arrest Roger Thomas Clark. Attached to that request were a criminal Complaint against Clark and an arrest warrant, both issued in this District. (Dkt. 1 (15 Mag. 1335)). The Complaint made plain that this was a computer crime. For instance, the Complaint explained that the charges related to Clark's various roles in the Silk Road, "an underground website" that "hosted a sprawling black-market bazaar on the Internet, where illegal drugs and other illicit goods and services were regularly bought and sold by the site's users." The Complaint also noted that Clark (1) "hir[ed] and manag[ed] a computer programmer who assisted in developing computer code and maintaining Silk Road's technical infrastructure"; (2) provided "advice to Ulbricht regarding managing and operating Silk Road, including security advice"; (3) assisted in "promoting sales on the Silk Road website; and (4) conducted "research and collect[ed] intelligence on the efforts of law enforcement to investigate Silk Road." Finally, the Complaint noted that law enforcement recovered, from Ulbricht's laptop computer, "over a thousand pages of chats between Ulbricht and "VJ" and "Cimon"; the Complaint supplied examples of a number of these chats about a host of topics, including a chat in which Clark recommended security improvements to the Silk Road website.

On or about December 3, 2015, the Royal Thai Police arrested Clark in his home on Koh Chang Island in Thailand. In connection with Clark's arrest, the Royal Thai Police seized various electronic devices from Clark's home (the "Thai Devices"), an unsurprising fact in a computer

crime case.[20] Clark has not alleged that U.S. law enforcement participated in his arrest, or in the seizure of the Thai Devices, in any way, nor does the Government have any information to suggest any involvement or direction by U.S. law enforcement.

The Thai Devices were later supplied to U.S. law enforcement in response to a post-arrest MLAT request, and subsequently searched pursuant to a judicially authorized search warrant signed in this District.[21]

2. Discussion

The United States submitted a request to the Kingdom of Thailand to arrest a defendant in a sophisticated cybercrime case. The Royal Thai Police, acting alone, arrested the defendant in his home; they also seized the Thai Devices—an unsurprising fact in a case involving computer crime. The Government later obtained a judicially authorized search warrant in this District that did not rely, in any way, on the consent form. That ends the matter. As noted above, the Silk Road website operated online, required access through the Tor browser, and required payment through electronic currency (Bitcoin); thus, anyone involved in Silk Road (such as Clark) necessarily used electronic devices. It is eminently reasonable for foreign law enforcement officers to seize a cyber-defendant's devices in connection with his arrest—especially where (as here) those devices were not searched before a judicially authorized warrant was obtained.

[20] Three of the Thai Devices are encrypted computers. At this time, the Government has not been able to access the contents of these three computers, though the Government's efforts to decrypt the devices is ongoing.

[21] Unlike the Icelandic Server, the Thai Devices were *not* imaged or accessed overseas. Although, consistent with *Verdugo-Urquidez*, a warrant was not necessary to search these devices belonging to a foreign national with no ties to the United States after they were seized by foreign law enforcement abroad, the Government obtained a search warrant out of an abundance of caution.

The defendant contends that the "case law that has developed in the related context of a defendant seeking to suppress a coerced statement is instructive. One of the justifications for excluding confessions that were induced by physical or psychological compulsion is the concern that a statement obtained through those might not be true." (Def. Br. 40). Such concerns plainly are not at issue here, given that (1) the Government did not rely on the consent form in obtaining a search warrant; (2) the Government will not rely on the consent form in its case-in-chief at trial; and (3) such concerns do not affect, in any way, the reliability or accuracy of electronic devices recovered from a cyber-defendant's home. In any event, the defense's focus on cases in which defendants sought to suppress an allegedly coerced statement is unavailing, for the law requires far more than even Clark's uncorroborated claims. *See, e.g.*, *United States v. Salameh*, 152 F.3d 88, 117 (2d Cir. 1998) (holding an accused's statement to be voluntary where, prior to being taken into U.S. custody, he had been incarcerated in Egypt and tortured for ten days); *Campaneria v. Reid*, 891 F.2d 1014, 1020 (2d Cir. 1989) (holding that interrogation was not coercive where the defendant was young, foreign-born with a poor command of English, "suffering from a serious knife wound and was in significant pain," and "questioned while in the ICU with tubes running in and out of his body").

V. CLARK'S DISCOVERY REQUESTS SHOULD ALL BE DENIED

Notwithstanding the extensively developed record in this case and the prior *Ulbricht* prosecution, Clark essentially reincorporates Ulbricht's sweeping discovery requests "relat[ing] to the manner in which Agent Tarbell and another member of the CY-2 squad located the Silk Road IP address in 'early June' of 2013." (Def. Br. 33). Clark, like Ulbricht before him, has failed to make any specific showing of materiality that would justify these requests, and they should therefore be denied.

Clark's discovery requests are based on the imaginative theory that his Fourth Amendment rights were somehow violated by an unspecified government agency—as opposed to a competent showing of materiality. A defendant bears the burden of making a *prima facie* showing that any documents he seeks under Rule 16(a)(1)(E) are material to preparing the defense. *United States v. Maniktala*, 934 F.2d 25, 28 (2d Cir. 1991); *United States v. McGuinness*, 764 F. Supp. 888, 894 (S.D.N.Y. 1991). To satisfy this burden, the defendant "must offer more than the conclusory allegation that the requested evidence is 'material.'" *United States v. Ashley*, 905 F. Supp. 1146, 1168 (E.D.N.Y. 1995) (citing *McGuinness*, 764 F.Supp. at 895). Similarly, "basing discovery requests on nothing more than mere conjecture" is a "non-starter." *United States v. Persico*, 447 F. Supp. 2d 213, 217 (E.D.N.Y. 2006) (rejecting discovery request for "long list of items," where "[t]he theme underlying these requests is that only Defendants, upon review of the requested material, will be able to discern whether or not impeachment or exculpatory information is embedded therein," adding: "[T]he criminal pretrial discovery process does not work that way.").

The Government has explained how the FBI was able to locate the Icelandic Server, and it has already explained at length how Ulbricht was identified as "DPR." There is therefore no basis for Clark to go on a "blind and broad fishing expedition" for proof of some darker, alternative storyline, somehow involving violations of his Fourth Amendment rights, when there isn't a shred of evidence that any such violations actually happened. *United States v. Larranga Lopez*, 05 Cr. 655 (SLT), 2006 WL 1307963, at *7-*8 (E.D.N.Y. May 11, 2006) (Rule 16 "does not entitle a criminal defendant to a 'broad and blind fishing expedition among [items] possessed by the Government on the chance that something impeaching might turn up'" (quoting *Jencks v. United States*, 353 U.S. 657, 667 (1957)); *see also United States v. Wilson*, 571 F. Supp. 1422, 1424 (S.D.N.Y. 1983) (rejecting discovery motion where its "wide-ranging scope suggests that the

defendant is not seeking information to which he is entitled under the discovery rules to enable him to defend against the current charge, but that he is engaged upon a fishing expedition which, if permitted, would in effect require the government to disgorge material contained in its internal investigatory files").[22]

Because Clark has not established that he has a reasonable expectation of privacy in the Icelandic Server—or standing to assert any claims in its foreign search under the Fourth Amendment—his motion should be denied. *See United States v. Ulbricht*, No. 14 Cr. 68 KBF, 2014 WL 5090039, at *4 (S.D.N.Y. Oct. 10, 2014), *aff'd*, 858 F.3d 71 (2d Cir. 2017) (denying Ulbricht's motions for discovery into the manner the Icelandic Server was located and to suppress the server based on defendant's failure to establish a reasonable expectation of privacy in the

[22] Clark's discovery requests are improper for other reasons as well. For one thing, the requests are principally posed in the form of interrogatories, which are out of place in the criminal context. *See United States v. Conder*, 423 F.2d 904, 910 (6th Cir. 1970) ("By its very terms Rule 16[] is limited to inspection and copying of tangible objects. Clearly therefore, the interrogatories filed by the defendants here were not an appropriate mode of discovery . . . ."); *United States v. Cameron*, 672 F. Supp. 2d 133, 137 (D. Me. 2009) (rejecting criminal discovery demands that "sound more like civil interrogatories under civil Rule 33 than document requests under Rule 16(a)(1)(E)"); *United States v. Schluter*, 19 F.R.D. 415, 416 (S.D.N.Y. 1956) ("There is no counterpart in the Rules of Criminal Procedure providing for . . . interrogatories such as are permitted under . . . the Rules of Civil Procedure."). Moreover, even to the extent Clark's discovery requests could be construed as seeking documents, the documents that would be at issue—to the extent they existed—would consist largely or entirely of internal reports or other documents generated by agents or attorneys during the investigation, which are not subject to discovery under Rule 16. *See* Fed. R. Crim. P. 16(a)(2) (Rule 16 "does not authorize the discovery or inspection of reports, memoranda, or other internal government documents made by an attorney for the government or other government agent in connection with investigating or prosecuting the case"); *see also, e.g.*, *United States v. Batista*, 06 Cr. 265, 2009 WL 910357, at *10 (E.D.N.Y. Mar. 31, 2009) (denying defendant's request for "a variety of government and reports and records" sought in effort to collect evidence for suppression motion, holding that Rule 16(a)(2) "expressly prohibits such disclosures"); *see generally United States v. Armstrong*, 517 U.S. 456, 463 (1996) ("[U]nder Rule 16(a)(2), [a defendant] may not examine Government work product in connection with his case."); *United States v. Rufolo*, 89 Cr. 938 (KMW), 1990 WL 29425, at *1 (S.D.N.Y. Mar. 13, 1990) (holding Rule 16(a)(2) bars disclosure of investigative, agent, and surveillance reports prepared by federal agents).

Icelandic Server); *cf. Watson*, 404 F.3d at 167 (upholding denial of suppression motion without a hearing where defendant failed to proffer affidavit alleging possessory interest in premises searched); *United States v. Parilla*, No. 13 Cr. 360 (AJN), 2014 WL 1621487, at *5 (S.D.N.Y. Apr. 22, 2014) (denying motion to suppress fruits of vehicle search without a hearing where defendant had failed to show that he possessed "any property rights in the vehicle").

Even if Clark were to demonstrate that he has standing to challenge the search of the Icelandic Server, which he has failed to do, none of the discovery he seeks is related to any plausible violation of Clark's Fourth Amendment rights. Clark's motion, supported by the Declaration of Joshua Michel, claims that the "[t]he bulk of what is sought will help defense expert Joshua Michel reach a definitive conclusion on the validity of Agent Tarbell's claims" regarding the manner in which the Icelandic Server was identified. But in the next breath, the defense discloses that the expert has already reached the opinion that, purportedly, "it would have been implausible for Agent Tarbell to access the .49 server in the manner he claimed." (Def. Br. 35). At bottom, however, nothing in the Michel Declaration actually alleges that the Icelandic Server was either located or searched in a manner that violated the Fourth Amendment. It merely critiques certain aspects of the Tarbell Declaration concerning how the Icelandic Server was located. The Michel Declaration fails to allege *any* alternative explanation of how the Icelandic Server was located that, if proven, would establish that Clark's Fourth Amendment rights were somehow violated.[23] Thus, whatever quarrel Mr. Michel has with the Tarbell Declaration is irrelevant in the

[23] The only alternative version of events offered by the Michel Declaration is the assertion that when former Agent Tarbell typed the IP address of the Icelandic Server into an ordinary web browser—*after* he had already observed the IP address leaking from the Silk Road website—he should not have been able to access what Michel believes was the "back-end" part of the Silk Road marketplace website rather than the "front-end" of the website. Michel Decl. ¶¶ 15-30. Nothing about this technical dispute impacts the lawfulness of the initial identification of the IP address. The Government had ample reason to ask Icelandic authorities to search the Icelandic Server and,

absence of any competent, affirmative allegations of fact that could supply a basis for suppression if proven at a hearing. *See Parilla*, 2014 WL 1621487, at *5 (denying suppression motion where defendant merely argued that agent affidavit failed to adequately explain the circumstances leading to the seizure of the evidence at issue: "[W]ithout evidence showing that the search violated [defendant's] rights, there is no basis for suppression . . . [and] likewise no basis for [an] evidentiary hearing.").

The Tarbell Declaration makes clear that Special Agent Tarbell obtained the IP address of the Silk Road Website through closely examining traffic data received from the Silk Road website when he used a part of it that was fully accessible to the public at large—the login interface—and received error messages that were accessible to any user who entered erroneous login information. That is plainly not a search. In any event, because the Icelandic Server was located outside the United States, the Fourth Amendment would not have required a warrant, as explained above. *See Vilar*, 729 F.3d at 86; *In re Terrorist Bombings*, 552 F.3d at 167. At most, any search of the Icelandic Server needed only to be "reasonable"—that is, justified by "legitimate governmental interests." *Vilar*, 729 F.3d at 86.

The Government has already made extensive disclosures to Clark of materials properly subject to disclosure under Rule 16, including all the materials related to the Icelandic Server previously produced to Ulbricht. Indeed, the Government has gone well beyond its Rule 16

---

thus, to the extent the Fourth Amendment even applies to that search, it was plainly reasonable. FBI noticed that the IP address of the Icelandic Server had leaked from the Silk Road website (a vulnerability corroborated by Ulbricht in his own journal). Pen register data for the server collected by Icelandic authorities reflected a high volume of Tor traffic flowing to the server, consistent with it hosting a Tor hidden service. *See Watson*, 404 F.3d at 167 (upholding denial of suppression motion without hearing where "defendant failed to show that he could challenge the search under the Fourth Amendment, even assuming we credited the facts asserted in his counsel's affirmation").

obligations, producing to the defense—at the initial pretrial conference in June 2018—a binder consisting of much of the best "identity" evidence in this case (*i.e.*, a roadmap as to how the Government proves that Clark was "Variety Jones," "VJ," and "Cimon" on Silk Road). That decision is representative of how the Government has approached its discovery obligations throughout this case. For instance, in an abundance of caution, the Government made the entirety of a co-conspirator's device available to defense counsel, rather than risk that a pertinent file might be inadvertently omitted if the Government produced only a subset of files on that device. And an Assistant U.S. Attorney and FBI Special Agent repeatedly conducted telephonic troubleshooting for the defense from the FBI's offices, in order to ensure the defense could promptly access all previously produced discovery, including Silk Road servers.

Throughout discovery, which has consisted (to date) of approximately a dozen productions, the Government has made clear that it is aware of its continuing obligations to produce any exculpatory evidence in its possession, or any further material evidence within the parameters of Rule 16. There is no reason to doubt that the Government has acted in good faith. Accordingly, Clark's discovery requests should be denied. *See United States v. Savarese*, 01 Cr. 1121 (AGS), 2002 WL 265153, at *2 (S.D.N.Y. Feb. 22, 2002) ("To the extent [defendant] seeks more specific types of documents, the materiality of which he can articulate in more than a conclusory fashion, he may make a further request. Otherwise, the Court must, as always, depend upon the Government's good faith in complying with its obligations under Rule 16.").

VI. CONCLUSION

Clark's motions are all meritless and should be denied without a hearing.

Dated: New York, New York
December 12, 2019

Respectfully submitted,

GEOFFREY S. BERMAN
United States Attorney for the
Southern District of New York

By: _____/s/_____
Michael D. Neff
Vladislav Vainberg
Eun Young Choi
Assistant United States Attorneys
(212) 637-2107/1029/2187